

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Received & Inspected

Annual 64.2009(e) CPNI Certification for: 2015

MAR 07 2016

Date filed: 2/26/2016

FCC Mailroom

Name of company covered by this certification: East Coast Satellite Communications

Form 499 Filer ID: 830722

Name of signatory: Louis Altman

DOCKET FILE COPY ORIGINAL

Title of signatory: CEO

I, [REDACTED] cer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company [is] in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules [REDACTED]

The company [REDACTED] any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

If affirmative: [No actions taken against data brokers]

The company [REDACTED] ived any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

If affirmative: [REDACTED]

Signed Louis Altman

[electronic signature]

No. of Copies rec'd _____
List ABCDE _____

0

East Coast Satellite Communications CPNI Compliance Policy

CPNI Security Measures

GlobaFone does not allow on-line access to customer accounts. Therefore customers are not issued logins to access CPNI.

GlobaFone employees do not release CPNI information over the phone unless the customer can be clearly identified with a PIN or password. If the customer cannot provide a password or a PIN, information can only be mailed to the address on record or by the company calling the customer with the phone number on record.

If the customer is able to provide call detail information without GlobaFone employee assistance, then the GlobaFone employee is permitted to discuss call detail information with the customer.

GlobaFone does not have retail location and does not give out CPNI information at its place of business.

GlobaFone password protects access to internal record files and folders which contain CPNI.

Employee Training Policies

GlobaFone has instituted a program to oversee and supervise employees with access to CPNI.

GlobaFone employees will be reprimanded, suspended or terminated an employee for failing to follow CPNI procedures.

Use of CPNI in Marketing Campaigns

GlobaFone does not participate in third party marketing campaigns.

Advertising does not include CPNI.

GlobaFone does not provide on-line access to CPNI information, this notifying customers of their right to restrict access, the opt-in clause, opt out-clause and records for customer approval are not applicable.

Third party use of CPNI

GlobaFone does not allow third party access to CPNI information

Unauthorized access to CPNI

GlobaFone is committed to protecting all client information, including CPNI information. Any breach in access to information will be reported to the proper law enforcement authorities.

All records around the breach will be kept for a minimum of two years.